Утверждаю
директор СОШ №42
Джантаева Г.М.
09.09.2021г

Информационная безопасность

12.04.2019

В связи с развитием информационных технологий и компьютеризацией экономики одним из важнейших вопросов в деятельности компании становится обеспечение информационной безопасности.

Информация – это один из самых ценных и важных активов любого предприятия и должна быть надлежащим образом защищена.

Что обозначает понятие «информационная безопасность»?

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

1. **Конфиденциальность.** Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.

2. **Целостность.** Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.

3. **Доступность.** Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно.

Угрозы информационной безопасности

Угрозы информационной безопасности можно разделить на следующие:

- **Естественные** (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).

- **Искусственные,** которые также делятся на:
  - непреднамеренные (совершаются людьми по неосторожности или незнанию);
  - преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).

- **Внутренние** (источники угрозы, которые находятся внутри системы).

- **Внешние** (источники угроз за пределами системы)

Так как угрозы могут по-разному воздействовать на информационную систему, их делят на пассивные (те, которые не изменяют структуру и содержание информации) и активные (те, которые меняют структуру и содержание системы, например, применение специальных программ).

Наиболее опасны преднамеренные угрозы, которые все чаще пополняются новыми разновидностями, что связано, в первую очередь, с компьютеризацией экономики и распространением электронных транзакций. Злоумышленники не стоят на месте, а ищут новые пути получить конфиденциальные данные и нанести потери компании.

Чтобы обезопасить компанию от потери денежных средств и интеллектуальной собственности, необходимо уделять больше внимания информационной безопасности. Это возможно благодаря средствам защиты информации в лице передовых технологий.

Виды средств защиты информации :

Антивирусные программы — программы, которые борятся с компьютерными вирусами и возобновляют зараженные файлы.

- 

Облачный антивирус (CloudAV) – одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера. CloudAV – это также решение для эффективного сканирования вирусов на приспособлениях с невысокой вычислительной мощностью для выполнения самих сканирований. Некоторые образцы облачных антивирусных программ – это Panda Cloud Antivirus, Crowdstrike, Cb Defense и Immunet.

- 

Информация очень важна для успешного развития бизнеса, следовательно, нуждается в соответствующей защите. Особенно актуально это стало в бизнес-среде, где на передний план вышли информационные технологии. Так как мы живем в эпоху цифровой экономики, без них рост компании просто невозможен.

Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные компании.